

February 6, 2006
Via Electronic Filing

Ms. Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th St. SW
Washington DC 20554

RE: Access Point, Inc.

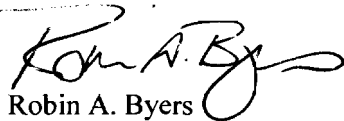
RE: Certification of CPNI Filing February 6, 2006, EB Docket No. 06-36; EB-06-TC-060

Dear Ms. Dortch:

Enclosed please find the following e-filing of the FCC Certification of CPNI Compliance for Access Point, Inc. In the following attachments, you will find all FCC requested documents necessary to complete CPNI compliance requirements pursuant to 47 CFR Section §64.2009, and Public Notice DA 06-223. No check is enclosed as no remittance fees are due.

Please address any inquiries or further correspondence regarding this filing to my attention at (919)851-4838.

Sincerely,



Robin A. Byers
Chief Operations Officer

Enclosure

cc: Craig Neeld, Technologies Management
cneeld@tminc.com

Byron McCoy, Telecommunications Consumers Division, Enforcement Bureau
Federal Communications Commission
Byron.mccoy@fcc.gov

Best Copy and Printing, Inc.
fcc@bcpiweb.com

**ANNUAL
OFFICER'S CERTIFICATION OF
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) COMPLIANCE**

I, Robin A. Byers, certify and state that:

1. I am the Chief Operations Officer of Access Point, Inc. and have personal knowledge of Access Point, Inc. operating procedures as they relate to CPNI, and the Rules and Regulations of the Federal Communications Commission regarding CPNI.
2. I hereby certify that, to the best of my knowledge, information and belief, Access Point, Inc. operating procedures are adequate to ensure compliance with its CPNI obligations pursuant to Section 222 of the Communications Act of 1934, as amended, and the Commission's rules found at 47 CFR Subpart U.
3. A further statement outlining the Access Point, Inc. operating procedures and compliance is attached as Exhibit A, as required by 47 C.F.R. §64.2009(e)

Robin A. Byers, Chief Operations Officer
Print Name and Title


Signature

2/06/2006
Date

Exhibit A:

Statement of CPNI Procedures and Compliance

Exhibit A.

RE: Access Point, Inc.

RE: Certificate of CPNI Filing February 6, 2006, EB Docket No. 06-36; EB-06-TC-060

Accompanying Statement to compliance certificate

The purpose of this statement is to provide a summary as to how Access Point, Inc.'s operating procedures ensure compliance with the rules contained in 47CFR § 64.2009; Safeguards required for use of customer proprietary network information.

The first Safeguard contained in 47CFR § 64.2009 states; (a) Telecommunications carriers must implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

Access Point, Inc. has created and maintains an electronic Customer Proprietary Network Information Approvals database that contains each customer that has given approval for use of their CPNI. This database is located in the company's Intranet website; InfoPoint. This intranet is available only to Access Point, Inc. employees. Each employee is assigned a unique login ID and password to access this intranet. When an employee separates from the company, their login and password are immediately disabled and access to the system is immediately denied. The Customer CPNI Approvals database is a view-only database to employees. Only those employees that are specifically authorized and have been assigned to maintain the database have other than view-only rights. These select employees each have a unique login ID and password which gives them system rights for database changes. All documented customer approvals for use of their CPNI are obtained from the customer in written form. These written approval documents are securely stored. An audit is conducted by Access Point, Inc. management personnel on a regular basis to affirm that the electronic Customer CPNI Approvals database is in exact conformity to the written approval document files.

The second Safeguard contained in 47CFR § 64.2009 states; (b) Telecommunications carriers must train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place.

Access Point, Inc. provides training to its employees on authorized use of CPNI, both to new employees at the time of hire and to the general employee population on an ongoing basis. The company has established a written policy and processes for authorized use of CPNI. The policy is described in the company handbook, which is given to all employees at the time of hire and is published on the company's Intranet. The policy specifically requires all employees to use the Customer CPNI Approval database to determine if a certain customer has given approval to use CPNI in all situations that require such approval, prior to use of that customer's CPNI. The process documents are used during training on authorized use of CPNI and are published on the company's Intranet. The company also has established policy and procedures for processing requests from outside entities for its customer CPNI, including subpoena requests by government agencies. Access Point, Inc. has a specific disciplinary process in place for unauthorized use of CPNI, which is published in the company handbook and is reviewed with each new employee at the time of hire. Unauthorized use of a customer's CPNI is deemed to be, and is stated in the handbook as, a terminable offense.

The third Safeguard contained in 47CFR § 64.2009 states; (c) All carriers shall maintain a record, electronically or in some other manner, of their own and their affiliates' sales and marketing campaigns that use their customers' CPNI. All carriers shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record

must include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. Carriers shall retain the record for a minimum of one year.

Access Point, Inc. does not use CPNI in the normal course of business for sales and marketing campaigns. However, if we were to do so, we would maintain records, stored electronically as well as in paper form for a period of no less than one year, of any and all of our sales and marketing campaigns that have used our customers' CPNI or in any case where CPNI has been disclosed or provided to third parties. Access Point Inc. does provide CPNI to a third party for purposes of bill presentment to our customers. In order to create and deliver monthly billing invoices we contract with a third party software and service company that provides our core telecom operations and billing support. Through this hosted service bureau environment, the order management and billing functions of our customer base are performed. Customer account records are initiated within this application, and all activity related to the customer records are maintained here. Access to this system is secured through username and password authentication and is restricted to authorized, trained company employees and critical third party support technicians. This system maintains a record of user logins to the application. As account activity occurs, the system maintains order history and event logs for audit and tracking purposes. These event records are maintained electronically for a minimum of one year. Access Point management has visibility into these event logs and can therefore track activity in the system. This third party billing provider is contractually bound to maintain the security and confidentiality of all of our customers' CPNI.

The fourth Safeguard contained in 47CFR § 64.2009 states; (d) Telecommunications carriers must establish a supervisory review process regarding carrier compliance with the rules in this subpart for outbound marketing situations and maintain records of carrier compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

Access Point, Inc. has established a supervisory review process. We have created an oversight committee consisting of senior operating managers that reviews the policies, systems, databases, stored documents, processes and policies on an ongoing basis to determine that we are in compliance with the rules for outbound marketing situations and that we are maintaining records of compliance for a minimum period of one year.

The fifth Safeguard contained in 47CFR § 64.2009 States; (e) A telecommunications carrier must have an officer, as an agent of the carrier, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. The carrier must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart.

Access Point, Inc. is complying with 64.2009(e) herein.

The sixth Safeguard contained in 47CFR § 64.2009 states; (f) Carriers must provide written notice within five business days to the Commission of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

(1) The notice shall be in the form of a letter, and shall include the carrier's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.

(2) Such notice must be submitted even if the carrier offers other methods by which consumers may opt-out.

Access Point, Inc. has not experienced any instance where an opt-out mechanism did not work properly. However, if such an instance shall occur, the company will provide written notice within five business days to the Commission. The company's oversight committee reviews this item on a regular basis.